

REMARKS

Claims 1-36 and 38-39 are pending.

Allowed Claims

The Examiner's indication that claims 8-12 are allowed is appreciated.

Claim Rejections Under 35 U.S.C. §103

The Examiner has presented a new ground of rejection. Claims 1, 3, 5-7 and 13-14, and 16-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,856,431 to Hirota et al. ("Hirota") in view of U.S. Patent No. 6,615,192 to Tagawa et al. ("Tagawa").

Claim 1 is reproduced below for convenience, and recites:

1. A method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising:
authorizing the media;
decrypting the track by a process comprising:
 - (a) calculating a media unique key; and thereafter
 - (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
 - (c) decrypting a group of frames; and thereafter
 - (d) deleting the decrypted title key;
 - (e) deleting the media unique key; and
 - (f) repeating (a) through (e) until the entire track is completed.

In the rejection of claim 1 based upon Hirota in view of Tagawa, the Examiner acknowledges that "Hirota does not explicitly disclose deleting the decrypted title key; and deleting the media unique key," but that "Tagawa in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed (Col.8, 56-61; Col. 11, lines 32-33). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota to include deleting the decrypted

title key and deleting the media unique key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Hirota (Col. 4, 17-19) in order to minimize the damage caused by the exposure of one of the encryption keys.” Office Action page 4.

It is kindly asserted that the combination of Hirota and Tagawa does not teach all of the elements of claim 1, as will be discussed below. It therefore cannot render the claim obvious.

Tagawa is cited for the proposition of teaching of steps (d) and (e) of the claim. Steps (d) and (e) are steps of an overall process of decrypting a track. Tagawa simply does not teach those steps, as will be discussed below. Further, it is well known that patentable combinations and processes often comprise individual elements or steps that may individually also be well known in the art. Even if the steps, taken individually, are well known, this does not render the combination as a whole obvious.

The relevant portion of Tagawa, as cited by the Examiner, relates to limiting copies of DVD Audio discs. It discloses a way to prevent a copy of DVD Audio disc made with a computer from being copied yet again. In summary, it prevents making a copy of a copy of the original disc. This is apparently done by deleting the title and disc keys so they are not written to the first copy of the DVD Audio disc. Therefore, a subsequent copy is prevented by a user who does not possess the original disc. The relevant portion of Tagawa is reproduced below.

The disc key is for decrypting the title key, and is a cipher key recorded on the DVD-Audio disc on which the content was originally recorded. Title and disc keys stored in the EEPROM 23 are deleted by the control microcomputer 26 when the limit set for the number of copies 1108 has been reached. Alternatively, the title and disc keys may be deleted whenever copying is performed by the disc drive 2. In the latter case, the title and disc keys must be obtained anew from the DVD-Audio disc each time the user wishes to make a copy, so that the user must have the original DVD-Audio disc in order to be able to make copies. As a result, copying by a user who does not possess an original disc can be prevented even if the number of copies has not reached its limit, and only copying made by the user in possession of the original disc authorized. Tagawa Col. 11, line 27-41.

This is not relevant to the process recited in claim 1 of:

decrypting the track by a process comprising:

- (a) calculating a media unique key; and thereafter
- (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
- (c) decrypting a group of frames; and thereafter
- (d) deleting the decrypted title key;
- (e) deleting the media unique key; and
- (f) repeating (a) through (e) until the entire track is completed.

To the contrary, the disclosure of Tagawa has to do with a way or mechanism of preventing repeated copying of a DVD audio disc. Tagawa does not teach a decrypted title key. Nor does Tagawa does teach or suggest decrypting a portion of a track (group of frames) at a time and thereafter deleting the keys that were necessary and then repeating all the steps until the entire track is completed. Furthermore, in addition to not teaching this, one of skill in the art would understand that the process Tagawa describes would not require or utilize a *decrypted* title key. This would explain why there is no disclosure in Tagawa of this. One of skill in the art would understand that the title key, if and when copied from the original to subsequent disc, would be in an *encrypted* format in order to minimize exposure of the key. In general, in such a copy operation disclosed by Tagawa, both the title key and the track would ideally be copied as encrypted, not decrypted. If they were decrypted for the copy operation they would be unnecessarily vulnerable.

Therefore, it is kindly submitted that independent claim 1, and all the claims that depend therefrom, is in condition for allowance.

Additionally, the dependent claims contain additional limitations not taught by the combination of Hirota and Tagawa and will be fully addressed if necessary if the rejection of maintained by the Examiner. In the meantime, the following is briefly offered in support of the claims dependent from claim 1.

The Examiner asserts that there is some teaching at Col. 59 of Tagawa that would render claim 3 obvious. Tagawa has only 18 columns so perhaps the Examiner intended to refer to Hirota at Col. 59. Nothing in Tagawa or Hirota in the cited area or otherwise teaches the

limitations of dependent claim 3 of “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key; and copying the singly encrypted title key from the media into a memory of the device.”

Independent claim 13 was rejected on the same basis as independent claim 1, and is therefore allowable, together with the claims that depend therefrom, for the same rationale given above regarding claim 1.

Claims 15 and 18-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hirota in view of Tagawa and further in view of U.S. Patent No. 5,790,423 to Lau et al. (“Lau”).

Claim 15 depends from claim 13 and adds a digital signal processor (“DSP”). Claim 18 adds to that that “the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor,” and claim 19 adds to claim 18 that “the interface means is executed by the digital signal processor.”

The Examiner adds Lau to the combination of Hirota and Tagawa for the proposition of a digital signal processor and indicates with a sweeping generalization that one of skill in the art would be motivated to make the combination in order [not] to provide real time digital signal processing. While Lau does disclose a digital signal processor, Lau does not teach use of the DSP in any encryption or decryption operation. Therefore Lau does not teach “secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor” as required by claim 18.

Furthermore there is no motivation to combine Lau with the combination of Hirota and Tagawa. Again, lacks any teachings related to any encryption and/or decryption operation, including usage of its DSPs (111, and 44). The Examiner appears therefore to rely on impermissible hindsight in making such a combination.

Therefore it is kindly submitted that claims 15 and 18-19 are not rendered obvious by the combination of Hirota, Tagawa, and Lau, and are in condition for allowance

Claims 20-27, 28, and 38-39 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hirota in view of Tagawa and in view of U.S. Patent No. 5,805,821 to Saxena et al. (“Saxena”).

For reasons similar to those discussed with regard to claim 1, the combination of Hirota and Tagawa does not teach the limitation of claim 20 wherein “the security engine (a) decrypts one or more of the keys, (b) decrypts a portion of the encrypted content using the one or more decrypted keys, and (c) deletes the one or more decrypted keys, and (d) repeats (a) - (c) until all portions of the content are decrypted.”

As admitted by the Examiner, the combination also does not teach “an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium.” Therefore, the Examiner has added Saxena to the combination of Hirota and Tagawa.

While Saxena does disclose usage of an API, Saxena is not related to and does not teach “a system that enables a device to decrypt a file having encrypted content on a secure medium,” as recited in the preamble to claim 20. Further, Saxena does not teach or suggest usage of its API in conjunction with a security engine for decrypting encrypted content or in conjunction with a secure system generally; there is no teaching of encryption or decryption with Saxena. Saxena relates to a video optimized media streamer user interface employing non-blocking switching to achieve isochronous data transfers. While Saxena mentions usage of an API, this is an insufficient motivation to combine. There are no specific teachings that would lead one of skill in the art to combine the teachings of all three of these references to arrive at the claimed combination. To the contrary, the Examiner appears to have used the claim itself as a roadmap, having picked and chosen elements from the prior art in order to arrive at the claimed combination. In short, the combination appears to hinge on hindsight.

Therefore, it is kindly submitted that claims 20-27, 28, and 38-39 are in condition for allowance.

Claims 26, and 29-32 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hirota in view of Tagawa and in view of Saxena and further in view of Lau.

Claims 26 and 29-32 depend from claim independent claim 20 and are allowable for all the reasons given above. Claim 26 adds a digital signal processor to claim 20, and claims 29-32 recite further limitations relating the DSP. Therefore, Lau is added to the already tenuous combination of Hirota, Tagawa, and Saxena for the proposition of the DSP. Again, While Lau

does disclose a digital signal processor, Lau does not teach use of the DSP in any encryption or decryption operation or the use of the DSP in conjunction with or for execution of a security engine. Therefore, the combination of Hirota, Tagawa, Saxena and Lau does not teach all of the elements of these claims. Furthermore, this four way combination relies on hindsight and would be made by one of skill in the art. It would not be made without the benefit of the roadmap provided by the claim itself. Again, Lau does not teach use of the DSP in any encryption or decryption operation or the use of the DSP in conjunction with or for execution of a security engine.

Claim 3 is rejected under 35 U.S.C. §103(a) as being unpatentable over Hirota in view of Tagawa and further in view of U.S. Patent No. 6,367,019 to Ansell et al. ("Ansell").

Claim 3 was also initially rejected as obvious by the combination of Hirota and Tagawa. As discussed above, the combination of Hirota and Tagawa does not teach all of the elements of the claim and does not render the claim obvious. The addition of Ansell to the group does not remedy those shortcomings.

The Examiner indicates that "Both references [Hirota and Tagawa] do not explicitly disclose decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. Ansell, in analogous art, however, discloses decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key (Col.7, line 19)." Office action at page 14.

Ansell simply does not teach that. To the extent that Ansell teaches decrypting any doubly encrypted key, it would be the media master key of Ansell, not the claimed title key. Col. 7, line 14 to line 28 of Ansell illustrates this and is reproduced below.

The master media key is encrypted using the storage key of the particular external player to which SPT 116 is to be bound. To avoid divulging the storage key to player 110, the particular external player, rather than player 110, encrypts the master media key. Thus, in step 604 (FIG. 6), player 110 (FIG. 1) encrypts the media master key using a session key formed at the onset of a secure communication session between player 110 and portable player 150 and sends the encrypted master media key to portable player 150. Portable player 150 decrypts the master media key and re-encrypts the master media key using the storage key,

e.g., read-only key 504A and sends the encrypted master media key back to player 110. As a result, only portable player can decrypt the encrypted master media key and therefore the content of SPT 116.

Thus, contrary to the Examiner's assertion, the combination of Tagawa, Hirota, and Ansell does not teach all the elements of dependent claim 3, and cannot render the claim obvious.

Claims 33-37 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hirota in view of Tagawa in view of Saxena and further in view of Turgeon, U.S. Publication No. 2003/0014371.

Claim 33 in dependent and recites "the system of claim 20, further comprising:

one or more engines for processing and transmitting audio, video or images, each engine comprising a secure application programming interface, the secure interface(s) for accessing the encrypted content and keys of the medium:

wherein each of the one or more engines for processing and transmitting audio, video or images further comprises a non-secure application programming interface for accessing unencrypted content of the medium."

Claims 33-37 depend from independent claim 20 and are allowable for all reasons discussed with regard to that claim. Furthermore, these claims are allowable for the following additional reasons. The Examiner relies on Turgeon paragraph 12 as teaching "non-secure interface(s) for accessing the unencrypted content of the medium" of claim 33. While Turgeon does disclose accessing both encrypted and unencrypted content relating to a user's financial data, there is no teaching of an application programming interface or "API" for doing so. An API is not a user interface, but a *programming* interface to simplify software integration. An API is also not an inherent portion of every software program, or intelligent device utilizing some form of software logic.

Furthermore, the Examiner's contention that Turgeon is analogous art is contested. Turgeon is not pertinent to the problem at hand, and one of skill in the art would not look to Turgeon. Turgeon is primarily concerned with financial transactions and e-commerce and has little if anything to do with playing back recorded audio, video, or other content.

In addition, even if Turgeon is considered analogous art, one of skill in the art would not make a four (4) way combination of Hirota, Tagawa, Saxena, and Turgeon to arrive at the claimed invention without the benefit of hindsight. As discussed previously, there is no proper motivation to combine Hirota, Tagawa and Saxena in a three (3) way combination, let alone Hirota, Tagawa, Saxena, and Turgeon in a four (4) way combination. It is a very tenuous assertion that one of skill in the art would take the teachings of Turgeon's financial transactions and ecommerce and combine it with the other three references "in order to make the system versatile by allowing access to demos and samples" as asserted by the Examiner on page 15 of the Office Action.

Claim 37 has been canceled and its limitations incorporated into claim 33.

It is kindly submitted that claims 33-36 are not obvious and are in condition for allowance.

Conclusion

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

Respectfully submitted,



James S. Hsue
Reg. No. 29,545

June 16, 2006

Date

PARSONS HSUE & DE RUNTZ LLP
595 Market Street, Suite 1900
San Francisco, CA 94105
(415) 318-1160 (main)
(415) 318-1162 (direct)
(415) 693-0194 (fax)